BUNDESREPUBLIK DEUTSCHLAND

10.11.03

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 54 324.0

Anmeldetag: 21. November 2002

Anmelder/Inhaber: Philips Intellectual Property & Standards GmbH, Hamburg/DE

(vormals: Philips Corporate Intellectual Property GmbH)

Bezeichnung: Elektronisches Speicherbauteil und Verfahren zum Betreiben desselben

IPC: G 11 C 29/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 21. Oktober 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Wehner

A 9161
06/00
EDV-L

ZUSAMMENFASSUNG

Elektronisches Speicherbauteil und Verfahren zum Betreiben desselben

Um ein elektronisches Speicherbauteil (100), aufweisend mindestens einen Speicherzellenbereich (10), der in mindestens ein dotiertes Aufnahmesubstrat (20) eingebettet und/oder eingelassen ist und in dem reguläre Daten repräsentierende physikalische Zustände (P) mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming Code, beschreibenden Abbildungsfunktion (A) abgebildet sind, sowie ein Verfahren zum Betreiben mindestens eines elektronischen Speicherbauteils (100) der vorgenannten Art so weiterzubilden, dass zum einen die Wahrscheinlichkeit einer Fehlererkennung deutlich erhöht ist und zum anderen unbeschriebene Speicherblöcke in zuverlässiger Weise von schon einmal beschriebenen Speicherblöcken unterschieden werden können, wird vorgeschlagen, dass mittels der Abbildungsfunktion (A) mindestens ein weiterer physikalischer Zustand in Form mindestens eines Ausnahmezustands (L, S) im Fehlerkorrekturcode erfasst, kodiert und/oder signalisiert werden kann.

Fig. 2

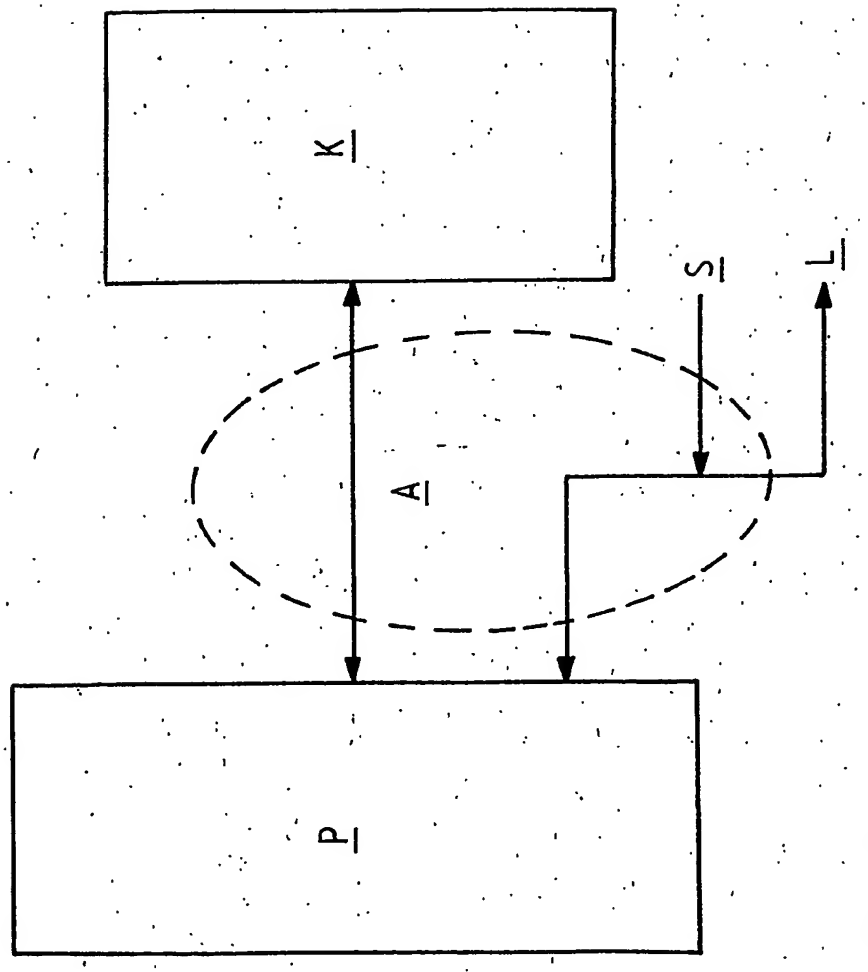

Fig.2

BESCHREIBUNG

Elektronisches Speicherbauteil und Verfahren zum Betreiben desselben

Die vorliegende Erfindung betrifft allgemein das technische Gebiet der elektronischen Bauteile, insbesondere der mikroelektronischen Bauteile.

Im speziellen betrifft die vorliegende Erfindung ein elektronisches Speicherbauteil, aufweisend mindestens einen Speicherzellenbereich, der in mindestens ein dotiertes Aufnahmesubstrat eingebettet und/oder eingelassen ist und in dem reguläre Daten repräsentierende physikalische Zustände mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming Code, beschreibenden Abbildungsfunktion abgebildet sind.

Im speziellen betrifft die vorliegende Erfindung des weiteren ein Verfahren zum Betreiben mindestens eines elektronischen Speicherbauteils der vorgenannten Art.

Elektronische Speicherbauelemente, wie zum Beispiel E[rasable] P[rogrammable] R[ead] O[nly]M[emories], E[lectrical]E[rasable] P[rogrammable]R[ead]O[nly]M[emories], Flash-Speicher, R[ead]O[nly] M[emories] oder R[andom]A[ccess]M[emories], erlauben das Lesen und/oder das Schreiben von digitalen Daten der Form "1" und "0", die häufig als geschriebener bzw. gelöschter Zustand (Bit) bezeichnet werden. Durch Abnutzung, durch äußere Einflüsse oder durch andere Ursachen kann es gelegentlich zu einem fehlerhaften Lesen dieser Daten kommen.

Diesem fehlerhaften Lesen der Daten kann zum Beispiel durch den Einsatz eines Fehlerkorrekturcodes entgegengewirkt werden, bei dem die Information redundant auf dem physikalischen Medium abgespeichert wird und ein Algorithmus beim Einlesen der Daten eben diese Daten auf Fehler hin untersucht.

Typischerweise werden Algorithmen verwendet, die in einem Speicherblock von zum Beispiel acht logischen Bits (, denen dann mehr als acht physikalische Bits entsprechen,) ein oder mehrere fehlerhafte Bits erkennen und/oder korrigieren können. Die Zuordnung der physikalisch gespeicherten Bits P (= physikalische Repräsentation) eines Speicherblocks zu den logisch ausgelesenen Bits K (= Benutzerrepräsentation) des Speicherblocks wird als Abbildungsfunktion A des Fehlerkorrekturcodes bezeichnet.

In Figur 1 ist in schematischer Blockdarstellung der von der Abbildungsfunktion A des Fehlerkorrekturcodes vermittelte konventionelle Zusammenhang gemäß dem Stand der Technik zwischen den physikalisch implementierten Bits P und den für den Benutzer verfügbaren, gegebenenfalls fehlerkorrigierten Bits K dargestellt. Bekannte Beispiele für derartige Fehlerkorrekturcodes sind Hamming Codes.

Aus Effizienz- und Kostengründen kann der zur Fehlererkennung verwendete Algorithmus niemals alle prinzipiell möglichen Fehler erkennen, sondern ist immer auf die Erkennung und eventuelle Korrektur von relativ wenigen Bits pro Speicherblock beschränkt. Diese konventionelle fehlertolerante Kodierung der Daten reicht in sicherheitskritischen Anwendungen nicht immer aus, insbesondere dann nicht, wenn einige charakteristische Fehlermuster in den Bits sehr viel häufiger als andere Fehlermuster auftreten oder auch sich durch externe Manipulation gezielt herstellen lassen.

So muss zum Beispiel bei der Kodierung des Zählers für das auf einer Geldkarte eingetragene Geld immer darauf geachtet werden, dass der physikalisch stabile Zustand, das heißt der Zustand, in den der Datenspeicher durch physikalische Prozesse nach einer Vielzahl von Jahren kippen könnte, einem leeren Kontostand entspricht, damit die Geldkarte nicht unbefugterweise mit mehr Geld nachgeladen werden kann.

Auch ist es mit dem Stand der Technik nicht einfach realisierbar, unbeschriebene Speicherblöcke von schon einmal beschriebenen Speicherblöcken zu unterscheiden. Dies ist beispielsweise im Bereich der Smart Cards ein potentielles Sicherheitsrisiko.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein elektronisches Speicherbauteil der eingangs genannten Art sowie ein diesem elektronischen Speicherbauteil zugeordnetes Verfahren der eingangs genannten Art so weiterzubilden, dass zum einen die Wahrscheinlichkeit einer Fehlererkennung deutlich erhöht ist und zum anderen unbeschriebene Speicherblöcke in zuverlässiger Weise von schon einmal beschriebenen Speicherblöcken unterschieden werden können.

Diese Aufgabe wird durch ein elektronisches Speicherbauteil mit den im Anspruch 1 angegebenen Merkmalen sowie durch ein Verfahren mit den im Anspruch 7 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den jeweiligen Unteransprüchen gekennzeichnet.

Gemäß der Lehre der vorliegenden Erfindung wird mithin ein völlig neuartiger Ansatz für einen mikroelektronischen Speicherbaustein mit redundanter Datenkodierung zum Erkennen und/oder zum Markieren von ungültigen oder anderweitig speziellen Zuständen offenbart.

Hierfür weist die den Fehlerkorrekturcode, zum Beispiel einen Hamming Code, beschreibende Abbildungsfunktion zumindest die spezielle Eigenschaft auf, dass es zusätzlich zum Abbilden sämtlicher "normalen", die regulären Daten repräsentierenden physikalischen Zustände im Speicher mindestens einen weiteren physikalischen Zustand gibt, der einen Ausnahmezustand darstellt und der anhand seines Bitmusters auf jeden Fall erkannt werden kann, unabhängig davon, ob für die "normalen" Zustände, das heißt für die regulären Daten nur eine eingeschränkte Fehlererkennung bzw. Fehlerkorrektur möglich sein sollte, oder ob die Fehlerkorrektur bzw. Fehlerverkennung für die normalen Zustände nicht eingeschränkt wird.

Zweckmäßigerweise wird dieser weitere physikalische Zustand (oder werden diese weiteren physikalischen Zustände) so gewählt, dass unvermeidlichen physikalischen Einschränkungen des Speichermediums Rechnung getragen wird; so kann zum Beispiel in einem EEPROM der Zustand, in dem die Speicherzellentransistoren eines jeden Bits ausgeschaltet sind und nur Leckströme fließen, als ein spezieller Ausnahmezustand festgelegt werden. Die Implementierung des Fehlerkorrekturcodes und die möglichen Reaktionen auf die verschiedenen Zustände kann in Hardware oder in Software erfolgen.

Mit den vorbeschriebenen Maßnahmen ist es zum Beispiel möglich, einen Speicherblock als noch nicht beschrieben zu markieren, indem dieser Zustand als spezieller Ausnahmezustand im Fehlerkorrekturcode festgelegt wird. Im Beispiel der Geldkarte bietet es sich an, den physikalisch stabilen Zustand (, der sich nach vielen Jahren einstellen könnte, wenn keine Gegenmaßnahmen getroffen werden,) als "nicht beschrieben" zu definieren.

Gemäß einer bevorzugten Ausgestaltung der vorliegenden Erfindung können zudem alle weiteren physikalischen Zustände, die sich durch Manipulation des Speichers, wie zum Beispiel durch Bestrahlen mit elektromagnetischen Teilchen oder Wellen, auf relativ einfache Weise herstellen lassen, als Ausnahmezustände im Fehlerkorrekturcode gekennzeichnet werden. Diese Zustände können dann von der Software und/oder von der Hardware der Geldkarte eindeutig erkannt werden, so dass Manipulationen des Speichers entgegengewirkt werden kann.

Mit im wesentlichen der gleichen Methode lassen sich auch sicherheitsrelevante Daten oder Merkmale eines Chips schützen, zum Beispiel indem dieser Bereich so ausgelegt wird, dass im Normalbetrieb keine Ausnahmezustände auftreten können, dass aber andererseits zum Beispiel das Löschen eines Speicherblocks in diesem Bereich einen Ausnahmezustand generiert.

Dieser Ausnahmezustand in einem sicherheitsrelevanten Speicherbereich kann dann erkannt werden, woraufhin entsprechende Maßnahmen, wie etwa eine "hardware exception" oder Modus-Änderungen, durch die kontrollierende C[entral] P[rocessing] U[nit] ausgeführt werden, um die Sicherheit des gesamten Speicherinhalts und Chips zu gewährleisten. In besonders vorteilhafter Weise lassen sich durch diese Technik EEPROM-Fuses schützen (zum Beispiel Konfiguration- und Trimwerte), die unter anderem den Grad der Verriegelung eines SmartCard-Chips festlegen.

Im Rahmen der vorliegenden Erfindung ist es durchaus möglich, die Speicherblocks bewusst mit einem Ausnahmezustand zu beschreiben, zum Beispiel um sie als unbeschrieben zu markieren oder, wie im Falle des EEPROMs, um viele Blocks erst einmal schnell mit "Null" zu initialisieren. Dies hat den Vorteil, dass beim nachfolgenden Schreiben nur noch die Hälfte der Zeit benötigt wird, weil keine Vorinitialisierung mehr erforderlich ist. In einem solchen Fall existieren dann zum Beispiel zwei verschiedene, der Null entsprechende Zustände, nämlich der Ausnahmezustand "gelöscht" und das eigentliche Datum "Null"; beim Lesen verhalten sich diese beiden "Nullen" unterschiedlich.

Die vorliegende Erfindung betrifft des weiteren die Verwendung eines elektronischen Speicherbauteils gemäß der vorstehend dargelegten Art zum Erkennen und/oder zum Markieren von ungültigen oder anderweitig speziellen physikalischen Zuständen.

Die vorliegende Erfindung betrifft schließlich die Verwendung eines Verfahrens gemäß der vorstehend dargelegten Art zum Implementieren mindestens eines zusätzlichen Sicherheitsmerkmals in mindestens einer Smart Card.

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 sowie dem Anspruch 7 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend anhand des durch die Figuren 2 und 3 veranschaulichten Ausführungsbeispiels näher erläutert.

Es zeigt:

Fig. 1 in schematischer Blockdarstellung den von der Abbildungsfunktion des Fehlerkorrekturcodes vermittelten konventionellen Zusammenhang gemäß dem Stand der Technik zwischen den physikalisch implementierten Bits und den für den Benutzer verfügbaren, gegebenenfalls fehlerkorrigierten Bits;

Fig. 2 in schematischer Blockdarstellung ein Ausführungsbeispiel für eine Erweiterung des Fehlerkorrekturcodes aus Fig. 1 zum Erfassen eines oder mehrerer Ausnahmezustände gemäß der vorliegenden Erfindung; und

Fig. 3 in schematischer, aus Gründen der Übersichtlichkeit sowie der Erkennbarkeit der einzelnen Ausgestaltungen, Elemente oder Merkmale nicht maßstabsgerechter Querschnittsdarstellung ein Ausführungsbeispiel für ein mikroelektronisches Speicherbauteil gemäß der vorliegenden Erfindung.

Gleiche oder ähnliche Ausgestaltungen, Elemente oder Merkmale sind in den Figuren 1 bis 3 mit identischen Bezugszeichen versehen.

In Figur 2 ist ein Ausführungsbeispiel für ein Verfahren zum Betreiben eines elektronischen Speicherbauteils 100 gemäß Figur 3 dargestellt. Bei diesem Verfahren werden reguläre Daten repräsentierende physikalische Zustände P mittels einer einen Fehlerkorrekturcode, nämlich einen Hamming Code, beschreibenden Abbildungsfunktion A abgebildet.

Gemäß Figur 2 ist der Fehlerkorrekturcode nun dahingehend erweitert, dass auch Ausnahmezustände S, L im physikalischen Bereich erkannt werden und entsprechend darauf reagiert wird. So kann der Benutzer zum Beispiel den physikalischen Speicher(zellen)-bereich 10 mit dem Ausnahmezustand "gelöscht" beschreiben (--> Bezugszeichen S in Figur 2). Ein späteres Lesen (--> Bezugszeichen L in Figur 2) desselben Speicher-

bereichs 10 führt dann zu einer geeigneten Ausnahme (sogenannte "exception"), falls dieser Ausnahmezustand nicht zwischenzeitlich wieder mit regulären Daten überschrieben wurde. Dies zwingt den Benutzer zu einer logisch korrekten Reihenfolge der Schreibvorgänge (--> Bezugszeichen S in Figur 2) und der Lesevorgänge (--> Bezugszeichen L in Figur 2).

Die Implementation gemäß Figur 2 kann auch dazu genutzt werden, ein nicht-autorisiertes externes Löschen beispielsweise von EPROM- oder EEPROM-Speicherbausteinen, etwa mit U[ltra]V[iolett]-Licht, als Ausnahmezustand zu erkennen und dementsprechend zu reagieren.

Alternativ oder in Ergänzung hierzu kann die Implementation gemäß Figur 2 auch dazu genutzt werden, um bewusst Ausnahmezustände zu erzeugen, bei denen erst deren spätere Löschung das erfolgreiche Ende einer finanziellen Transaktion auf einer Geldkarte signalisiert.

Zusammenfassend lässt sich in bezug auf das Verfahren gemäß Figur 2 also feststellen, dass der Fehlerkorrekturcode exemplarisch erweitert ist, um einen oder mehrere Ausnahmezustände mitzuerfassen. Die "normalen" Daten des Benutzers schreibt und liest dieser in den Registern der gegebenenfalls fehlerkorrigierten Bits K. Der Benutzer hat aber auch die Möglichkeit, einen Ausnahmezustand selbst zu schreiben. In jedem Falle wird der Benutzer durch ein geeignetes Signal davon unterrichtet, wenn er beim Lesevorgang auf der Seite der physikalischen Bits P einen Ausnahmezustand vorfindet.

Beim anhand Figur 3 veranschaulichten Ausführungsbeispiel eines mikroelektronischen Speicherbausteins 100 auf Halbleiterbasis handelt es sich um einen Flash-Speicherbaustein mit in ein p-dotiertes Aufnahmesubstrat 20 in Form einer HPW-Wanne eingebetteter, das heißt eingelassener Speicherzelle(nmatrix) 10 gemäß der vorliegenden Erfindung.

Dieser Speicherzelle(nmatrix) 10 sind zwei außenliegende Quellen (= Sources) 12a, 12b, eine zentrale Bitline 14, eine zwischen Bitline 14 und erster Quelle 12a bzw. zweiter Quelle 12b angeordnete Wordline 16 sowie ein zwischen Bitline 14 und Wordline liegender Control Gate 18 zugeordnet.

Beim gezeigten Speicherbaustein 100 wird eine hohe Spannung zum Programmieren oder zum Löschen benötigt. Um in diesem Zusammenhang die maximal zu handhabende Spannung so gering wie möglich zu halten, wird die Programmierspannung in einen positiven Anteil und in einen negativen Anteil aufgeteilt. Dies führt dazu, dass das p-dotierte Aufnahmesubstrat 20, in dem die Speicherzellen 10 gebildet werden, auch an ein negatives Potential angeschlossen werden kann.

Mittels des mikroelektronischen Speicherbausteins 100, insbesondere mittels seiner Speicherzellen(matrix) 10 lässt sich das Verfahren gemäß Figur 2 verwirklichen.

BEZUGSZEICHENLISTE

100	elektronisches Speicherbauteil, insbesondere mikroelektronisches Speicherbauteil
10	Speicherzellenbereich oder Speicherzellenmatrix
12a	erste Quelle oder erste Source
12b	zweite Quelle oder zweite Source
14	Bitline
16	Wordline
18	Control Gate
20	Aufnahmesubstrat
A	Abbildungsfunktion eines Fehlerkorrekturcodes
K	Benutzerrepräsentation: korrigierte Bits oder logisch ausgelesene Bits
L	Lesen: Signal an Benutzer (zweiter Ausnahmezustand)
P	physikalische Repräsentation: physikalische Bits oder physikalisch gespeicherte Bits
S	Schreiben durch Benutzer (erster Ausnahmezustand)

PATENTANSPRÜCHE

1. Elektronisches Speicherbauteil (100), aufweisend mindestens einen Speicherzellenbereich (10), in dem reguläre Daten repräsentierende physikalische Zustände (P) mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming Code, beschreibenden Abbildungsfunktion (A) abgebildet sind,
gekennzeichnet durch,
mindestens einen weiteren, mindestens einen Ausnahmezustand (L, S) im Fehlerkorrekturcode darstellenden physikalischen Zustand.

2. Speicherbauteil gemäß Anspruch 1,
dadurch gekennzeichnet,
dass der Fehlerkorrekturcode und/oder die möglichen Reaktionen auf die verschiedenen physikalischen Zustände hardwaremäßig und/oder softwaremäßig implementiert sind.

3. Speicherbauteil gemäß Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass der Ausnahmezustand (L, S) im Fehlerkorrekturcode
- durch das Fließen von Leckströmen bei ausgeschalteten Speicherzellentransistoren eines jeden Bits;
- als noch nicht beschriebener Speicherblock oder Speicherzellenbereich (10);
- durch Manipulieren des Speicherzellenbereichs (10), etwa durch Bestrahlen des Speicherzellenbereichs (10) mit elektromagnetischen Teilchen oder Wellen; und/oder
- durch das Löschen eines Speicherblocks oder Speicherzellenbereichs (10)

gegeben ist.

4. Speicherbauteil gemäß mindestens einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass der Speicherzellenmatrix (10)
- mindestens eine Quelle oder Source (12a, 12b),
- mindestens eine Bitline (14),
- mindestens eine Wordline (16) und
- mindestens ein Control Gate (18)

zugeordnet ist,

5. Speicherbauteil gemäß mindestens einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass das Speicherbauteil (100) als E[rasable] P[rogrammable]R[ead]O[nly]M[emory], als E[lectrical]E[rasable] P[rogrammable]R[ead]O[nly]M[emory], als Flash-Speicher, als R[ead]O[nly]M[emory] oder als R[andom]A[ccess]M[emory] ausgebildet ist.

6. Verwendung eines elektronischen Speicherbauteils (100) gemäß mindestens einem der Ansprüche 1 bis 5 zum Erkennen und/oder zum Markieren von ungültigen oder anderweitig speziellen physikalischen Zuständen.

7. Verfahren zum Betreiben mindestens eines elektronischen Speicherbauteils, insbesondere gemäß mindestens einem der Ansprüche 1 bis 6, in dem reguläre Daten repräsentierende physikalische Zustände (P) mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming Code, beschreibenden Abbildungsfunktion (A) abgebildet werden,
dadurch gekennzeichnet,
dass mittels der Abbildungsfunktion (A) mindestens ein weiterer physikalischer Zustand in Form mindestens eines Ausnahmezustands (L, S) im Fehlerkorrekturcode erfasst, kodiert und/oder signalisiert werden kann.

8. Verfahren gemäß Anspruch 7,
dadurch gekennzeichnet,
dass der weitere physikalische Zustand anhand seines Bitmusters auch im Falle einer für die regulären Daten geltenden eingeschränkten Fehlererkennung bzw. -korrektur erfasst, kodiert und/oder signalisiert werden kann.

9. Verfahren gemäß Anspruch 7 oder 8,
gekennzeichnet durch,
mindestens eine redundante Datenkodierung.

10. Verwendung eines Verfahrens gemäß mindestens einem der Ansprüche 7 bis 9 zum Implementieren mindestens eines zusätzlichen Sicherheitsmerkmals in mindestens einer Smart Card.

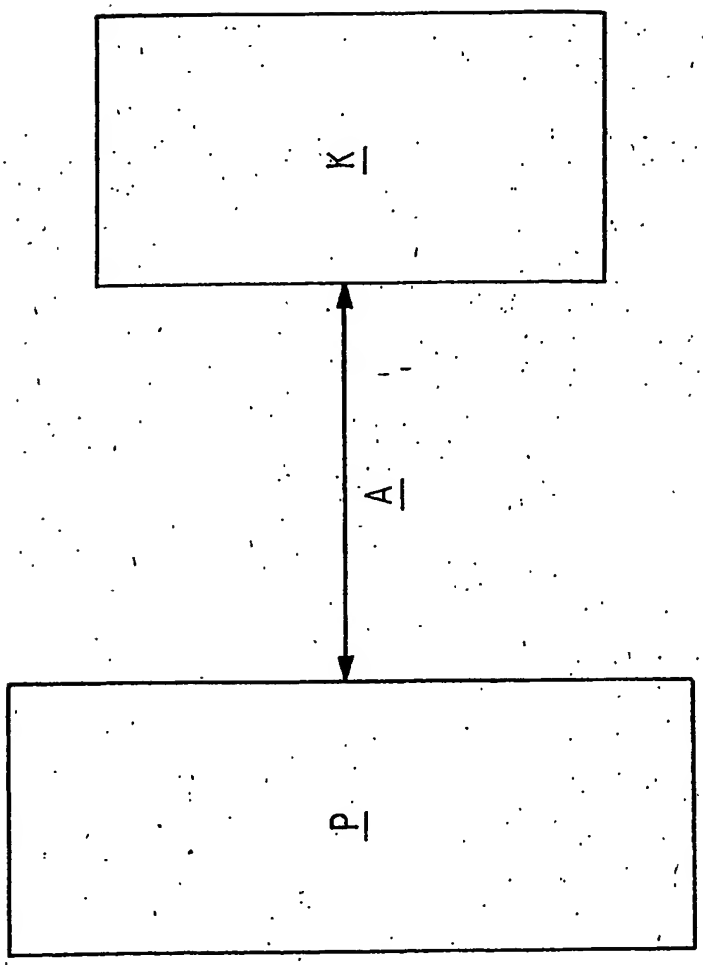

Fig.1

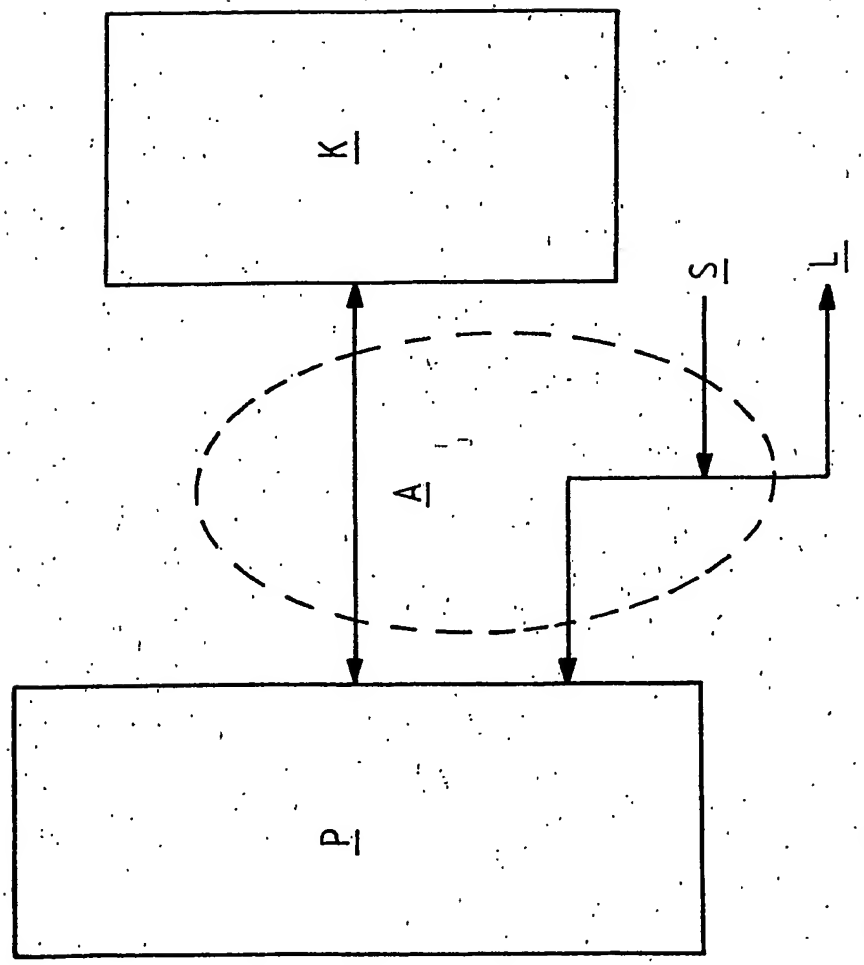

Fig.2

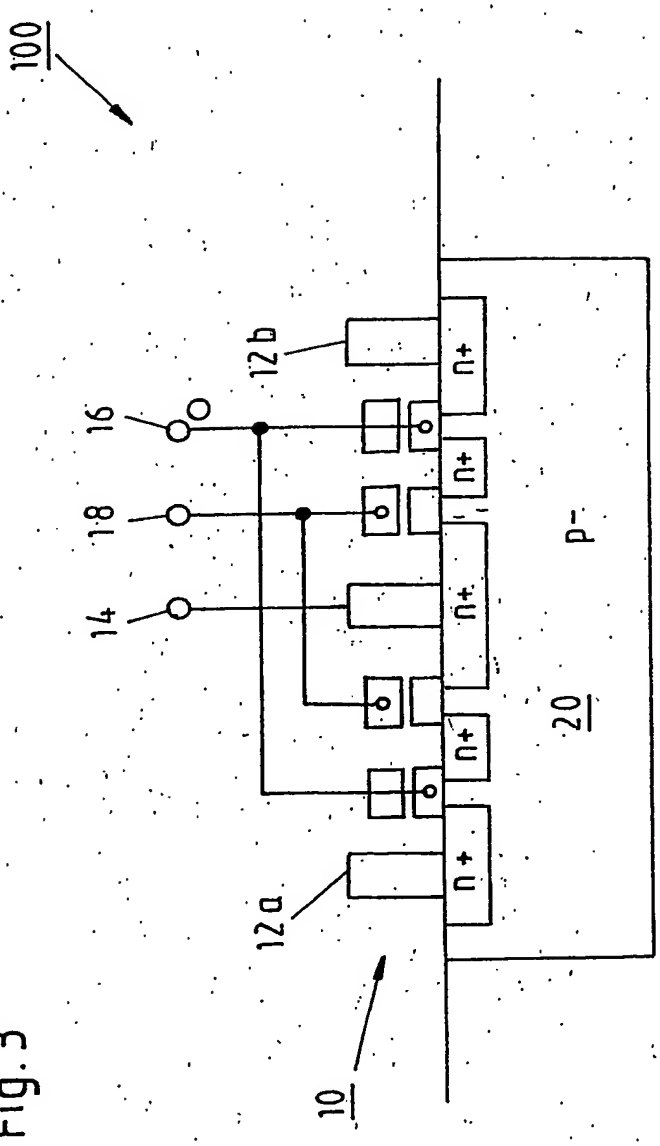

Fig. 3